

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-259305

(43)Date of publication of application : 13.09.2002

(51)Int.Cl.

G06F 13/00
H04L 12/58
H04N 1/00
H04N 1/32
H04N 1/44

(21)Application number : 2001-056607

(71)Applicant : MATSUSHITA GRAPHIC COMMUNICATION
SYSTEMS INC

(22)Date of filing : 01.03.2001

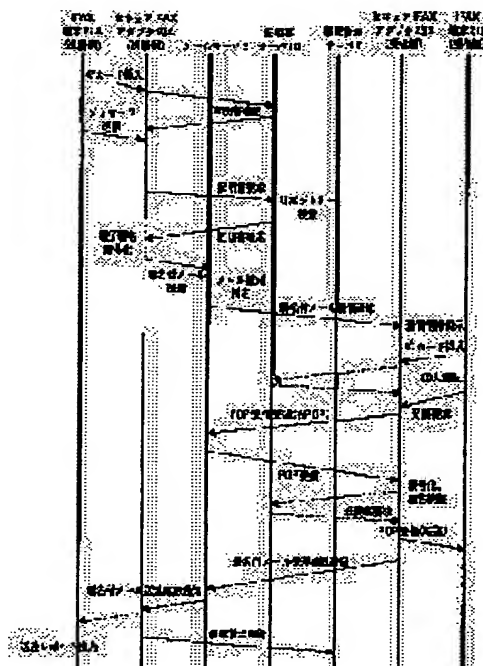
(72)Inventor : TOYODA KIYOSHI
MURATA MATSUHISA
AKIMOTO MASAO

(54) CIPHERED MAIL DISTRIBUTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a ciphered mail distribution system capable of attaining the conflicting requirements of high secrecy and the urgent distribution of a confidential document.

SOLUTION: When receiving a mail with a signature, a mail server 9 transmits a call income information mail to a secure IFAX adapter 23B on a receiving side to which the receiving person of the mail with the signature is registered. When receiving the call income information mail, the adapter 23B on the receiving side informs the receiving person being the owner of its destination account of the call-incoming of the ciphered mail from the destination account, requests the personal authentication of the receiving person by using an IC card 109 and receives/deciphers the mail with the signature after confirming the receiving person. Thus, the receiving person can fetch the confidential document of the mail with the signature speedily and surely from the server 9.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's
decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

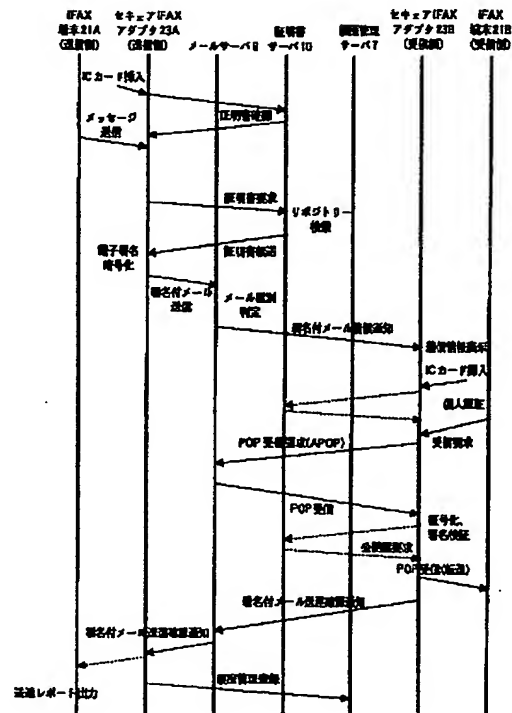
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of
rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY



【特許請求の範囲】

【請求項 1】 電子メールに暗号化処理を施して暗号化メールとして送信する電子メール送信端末装置と、前記暗号化メールの宛先としての電子メール受信端末装置と、受信した電子メールを宛先毎に蓄積される電子メール受信端末装置からの要求に応じて当該電子メール受信端末装置宛ての電子メールを送信する電子メールサーバ装置と、で構成される暗号化メール配信システムであつて、

前記電子メールサーバ装置は、前記暗号化メールを受信したならば前記暗号化メールの受信者が登録された電子メール受信端末装置に対して前記暗号化メールが着信した旨を通知する着信通知メールを直接送信する着信通知手段を具備し、

前記電子メール受信端末装置は、前記電子メールサーバ装置から着信通知メールを受信したならば前記受信者に対して前記暗号化メールの着信を通報する着信通知通報手段と、前記受信者の個人認証を行う個人認証手段と、前記個人認証手段によって前記受信者の確認が完了した後に前記暗号化メールの送信を前記電子メールサーバ装置に対して要求する電子メール受信手段と、前記電子メールの暗号化されたメッセージを復号化する復号化手段と、を具備することを特徴とする暗号化メール配信システム。

【請求項 2】 電子メール受信端末装置は、ICカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ICカードから読み出した情報を用いて個人認証を行うことを特徴とする請求項 1 記載の暗号化メール配信システム。

【請求項 3】 電子メール受信端末装置は、ICカードから情報を読み出すカードリーダ手段をさらに具備し、復号化手段は、前記ICカードに格納された受信者の秘密鍵を用いて暗号化メールの復号化処理を行うことを特徴とする請求項 1 記載の暗号化メール配信システム。

【請求項 4】 個人認証手段は、ICカードに格納された受信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記受信者が正常であることを確認することを特徴とする請求項 2 または請求項 3 記載の暗号化メール配信システム。

【請求項 5】 電子メール送信端末装置は、送信者の個人認証を行う個人認証手段をさらに具備し、前記個人認証手段により送信者の個人認証の確認が終了した後、電子メールを暗号化し電子メールサーバ装置に送信することを特徴とする請求項 1 から請求項 4 のいずれかに記載の暗号化メール配信システム。

【請求項 6】 電子メール送信端末装置は、ICカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ICカードから読み出した情報を用いて個人認証を行うことを特徴とする請求項 5 記載の暗号化メール配信システム。

【請求項 7】 電子メール送信端末装置は、証明書サーバから受信者情報を読み出す手段を具備し、暗号化手段は、前記受信者情報の公用鍵を用いて電子メールの暗号化処理を行うことを特徴とする請求項 5 記載の暗号化メール配信システム。

【請求項 8】 個人認証手段は、ICカードに格納された送信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記送信者が正常であることを確認することを特徴とする請求項 6 または請求項 7 記載の暗号化メール配信システム。

【請求項 9】 電子メール受信端末装置は、暗号化メールを受信後、送達確認通知を電子メール送信端末装置に送信することを特徴とする請求項 1 から請求項 8 のいずれかに記載の暗号化メール配信システム。

【請求項 10】 電子メール送信端末装置は、送達確認通知を受信したならばその内容を出力する出力手段を具備することを特徴とする請求項 9 記載の暗号化メール配信システム。

【請求項 11】 出力手段は、送達確認通知が所定の数だけ受信したならばそれらの内容をまとめて出力することを特徴とする請求項 10 記載の暗号化メール配信システム。

【請求項 12】 電子メール送信端末装置は、送達確認通知を受信したならば、履歴管理サーバに暗号化メールの送信履歴を登録することを特徴とする請求項 9 から請求項 11 のいずれかに記載の暗号化メール配信システム。

【請求項 13】 送信元の電子メール送信端末装置からの電子メールを配信するメールサーバ装置であつて、前記電子メールを蓄積する蓄積手段と、前記蓄積手段に蓄積した電子メールが所定の電子メールである場合には当該所定の電子メールの宛先に対して着信通知を行う通知手段と、前記宛先から要求があったならば前記蓄積手段に蓄積した前記所定の電子メールを前記宛先に送信する送信手段と、を備えることを特徴とするメールサーバ装置。

【請求項 14】 所定の電子メールは、送信元で電子メールに署名処理を施した署名付きメールであることを特徴とする請求項 13 記載のメールサーバ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号化メール配信システムに関する。

【0002】

【従来の技術】近年、一般的なファクシミリと同様の操作で画情報をインターネット経由で送信するファクシミリ装置が開発されている。この種のファクシミリは、通信経路の全部または一部にインターネットを使用することからインターネットファクシミリ端末装置（以下、「IFAX 端末」という）と呼ばれている。

【0003】このような I F A X 端末は、ファクシミリデータを電子メールのフォーマットに変換して送信する。具体的には、I F A X 端末は、読み取った原稿を M H データに変換し、その M H データを T I F F ファイルに変換する。さらに、その T I F F ファイルをテキストコード変換し、そのテキストコード変換されたデータを M I M E 形式に従ったデータに変換して送信を行っている。

【0004】I F A X 端末は、一人の者が占有するというよりも職場において同一の部署に属する複数の者によって共用されるのが一般的である。また、I F A X 端末宛ての電子メールは、I F A X 端末が自動的に受信し、印刷するため、送信側が指定した特定の個人以外の目に触れるおそれがあるので、通常のパーソナルコンピュータ等の一人の者が占有するメール受信端末に比べて秘匿性が低いと考えられている。

【0005】秘匿性の向上を目的として、I F A X 端末に、電子メールの傍受、改竄およびなりすましを防止する技術として電子署名や情報暗号化の技術を採用することが行われている。このタイプの I F A X 端末を“セキュア (Secure) I F A X”と呼んでいる。従来のセキュア I F A X は I C カードリーダを搭載し、送信側で I C カードから電子署名や情報暗号化に必要な情報（例えば、公開鍵、秘密鍵など）を読み出し、これを用いて電子メールに電子署名処理または情報暗号化処理を施した後送信する。受信側では、電子メールで指示された個人が自己の I C カードをスロットに挿入し、これから読み出した公開鍵、秘密鍵などを用いて電子メールを復号化し、印刷する。このようにして、I C カードの所有者以外のものが電子メールを傍受することを防止している。

【0006】

【発明が解決しようとする課題】しかしながら、従来のセキュア I F A X においては、I C カードの所有者だけが電子メールの受信を行うことができるようにするために、I C カードに記憶した所有者のメールアドレスおよびパスワードを用いて P O P サーバにログオンし、所有者のセキュア I F A X から電子メールを受信することが考えられる。この場合、I C カードがスロットに挿入されていることがメール受信の必須条件となる。これでは、定期的に P O P サーバにアクセスし、最新のメールを受信するためには、I C カードを常時スロットに挿入していなくてはならない。これでは却って秘匿性が低下してしまうので、秘匿性を保ちながら機密文書ができる限り早くよりリアルタイムに受信することは難しい。また、I C カードなしで P O P サーバに接続可能とするために、セキュア I F A X 本体にメールアドレスおよびパスワードを格納する場合も同様に高度の秘匿性を達成し得ない。このように従来のセキュア I F A X では、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができない。

【0007】本発明は、かかる点に鑑みてなされたものであり、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができる暗号化メール配信システムを提供することを目的とする。

【0008】

【課題を解決するための手段】本発明は、上記課題を解決するために、電子メール送信端末装置が、電子メールに暗号化処理を施して暗号化メールとして送信し、電子メールサーバ装置は、暗号化メールを受信したならば暗号化メールの受信者が登録された電子メール受信端末装置に対して暗号化メールが着信した旨を通知する着信通知メールを直接送信し、電子メール受信端末装置は、電子メールサーバ装置から着信通知メールを受信したならば受信者に対して暗号化メールの着信を通報し、受信者の個人認証により受信者の確認が完了した後に暗号化メールの送信を電子メールサーバ装置に対して要求し、暗号化メールを受信し復号化することとした。これにより、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができる。

【0009】

【発明の実施の形態】本発明の第1の態様は、電子メールに暗号化処理を施して暗号化メールとして送信する電子メール送信端末装置と、前記暗号化メールの宛先としての電子メール受信端末装置と、受信した電子メールを宛先毎に蓄積しある電子メール受信端末装置からの要求に応じて当該電子メール受信端末装置宛ての電子メールを送信する電子メールサーバ装置と、で構成される暗号化メール配信システムであって、前記電子メールサーバ装置は、前記暗号化メールを受信したならば前記暗号化メールの受信者が登録された電子メール受信端末装置に対して前記暗号化メールが着信した旨を通知する着信通知メールを直接送信する着信通知手段を具備し、前記電子メール受信端末装置は、前記電子メールサーバ装置から着信通知メールを受信したならば前記受信者に対して前記暗号化メールの着信を通報する着信通知通報手段と、前記受信者の個人認証を行う個人認証手段と、前記個人認証手段によって前記受信者の確認が完了した後に前記暗号化メールの送信を前記電子メールサーバ装置に対して要求する電子メール受信手段と、前記電子メールの暗号化されたメッセージを復号化する復号化手段と、を具備する構成を採る。

【0010】本発明の第2の態様は、第1の態様において、電子メール受信端末装置は、I C カードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記 I C カードから読み出した情報を用いて個人認証を行うこととした。

【0011】本発明の第3の態様は、第1の態様において、電子メール受信端末装置は、I C カードから情報を読み出すカードリーダ手段をさらに具備し、復号化手段は、前記 I C カードに格納された受信者の秘密鍵を用い

て暗号化メールの復号化処理を行うこととした。

【0012】本発明の第4の態様は、第2、3の態様において、個人認証手段は、ICカードに格納された受信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記受信者が正常であることを確認することとした。

【0013】これらの構成により、電子メールサーバ装置は暗号化メールを受信したならば暗号化メールの受信者が登録された電子メール受信端末装置に対して暗号化メールが着信した旨を通知し、かつ、この通知を受けた電子メール受信端末装置は受信者に対して暗号化メールの着信を通知し、受信者の個人認証を行うことを要求し、受信者の確認が取れた後、暗号化メールを受信、復号化するので、暗号化メールの機密文書を電子メールサーバ装置から所望の受信者に迅速かつ確実に取り出させることができる。

【0014】本発明の第5の態様は、第1から第4の態様のいずれかにおいて、電子メール送信端末装置は、送信者の個人認証を行う個人認証手段をさらに具備し、前記個人認証手段により送信者の個人認証の確認が終了した後、電子メールを暗号化し電子メールサーバ装置に送信することとした。

【0015】本発明の第6の態様は、第5の態様において、電子メール送信端末装置は、ICカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ICカードから読み出した情報を用いて個人認証を行うこととした。

【0016】本発明の第7の態様は、第5の態様において、電子メール送信端末装置は、証明書サーバから受信者情報を読み出す手段を具備し、暗号化手段は、前記受信者情報の公用鍵を用いて電子メールの暗号化処理を行うこととした。

【0017】本発明の第8の態様は、第6または第7の態様において、個人認証手段は、ICカードに格納された送信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記送信者が正常であることを確認することとした。

【0018】これらの構成により、電子メール送信端末装置は、個人認証を行い、送信者の確認を取った後、電子メールを暗号化して宛先に送信するので、不正な送信者による機密文書の配信を未然に防止することができる。

【0019】本発明の第9の態様は、第1から第8の態様のいずれかにおいて、電子メール受信端末装置は、暗号化メールを受信後、送達確認通知を電子メール送信端末装置に送信することとした。

【0020】本発明の第10の態様は、第9の態様において、電子メール送信端末装置は、送達確認通知を受信したならばその内容を出力する出力手段を具備することとした。

【0021】本発明の第11の態様は、第10の態様において、出力手段は、送達確認通知が所定の数だけ受信したならばそれらの内容をまとめて出力することとした。

【0022】本発明の第12の態様は、第9から第11の態様のいずれかにおいて、電子メール送信端末装置は、送達確認通知を受信したならば、履歴管理サーバに暗号化メールの送信履歴を登録することとした。

【0023】これらの構成により、電子メール受信端末装置は、暗号化メールを正常に受信したならば、送達確認通知を電子メール送信端末装置に返し、電子メール送信端末装置はこれを出力したり、送信履歴を履歴管理サーバに登録するので、機密文書の配信があったことを送信者が確認したり、その後第三者などが送信履歴を容易に確認することができる。

【0024】本発明の第13の態様に係るメールサーバ装置は、送信元の電子メール送信端末装置からの電子メールを配信し、前記電子メールを蓄積する蓄積手段と、前記蓄積手段に蓄積した電子メールが所定の電子メールである場合には当該所定の電子メールの宛先に対して着信通知を行う通知手段と、前記宛先から要求があったならば前記蓄積手段に蓄積した前記所定の電子メールを前記宛先に送信する送信手段と、を備える構成を採る。本発明の第14の態様は、第13の態様において、所定の電子メールは、送信元で電子メールに署名処理を施した署名付きメールであることとした。

【0025】以下、本発明の実施の形態について図面を参照して詳細に説明する。図1は、本発明の一実施の形態に係る電子メール配信システムを示す概念図である。

【0026】この電子メール配信システム1は、一つの管区局3と、その管理下にある複数の本部A〜本部Cと、それぞれの本部の管理下にある複数の支部A1、A2、B1、B2、C1、C2とで構成されている。これらは、WAN5で接続されている。

【0027】管区局3には、履歴管理サーバ7、メールサーバ9、証明書サーバ10が設けられたLAN11が構築されている。また、各本部A〜Cには、メールサーバ9がそれぞれ設けられたLAN13、15、17がそれぞれ構築されている。これらのLAN11〜17は、ルーター19を介してWAN5に接続している。

【0028】本部A〜Cおよび支部A1〜C2には、それぞれIFAX端末21が設置され、それにはセキュアIFAXアダプタ23が接続されている。支部A1〜C2に設置されたセキュアIFAXアダプタ23は、ルーター19を介してWAN25に接続する。セキュアIFAXアダプタ23は、表示モニタ27、スピーカ29および表示灯31を備えている。

【0029】図2は、上記実施の形態に係るセキュアIFAXアダプタのハードウェア構成を示すブロック図である。セキュアIFAXアダプタ23において、中央処

理部(CPU)101は、各種プログラムを実行してセキュアIFAXアダプタ23の各部を制御する。ROM103は、CPU101が実行するプログラムを格納する。RAM105は、プログラムのデータ領域として使用されると共に、所定のデータを格納するメモリとして使用される。

【0030】ICカードREAD/WRITE部(以下、「ICカードR/W部」という)107は、図示しないICカードスロットに装着されたICカード109に所定のデータの書込み、あるいは、ICカード109に書込まれたデータの読取りを行う。

【0031】第1LANインタフェース(以下、「第1LANI/F」という)111は、LAN11~17とのデータの送受信を制御するインタフェースである。LAN11~17に代わってルーター19に直接接続されても良い。第2LANインタフェース(以下、「第2LANI/F」という)113は、IFAX端末21とのデータの送受信を制御するインタフェースである。

【0032】外部入出力インタフェース(以下、「外部I/O」という)115は、表示モニタ27、スピーカ29および表示灯31に接続するためのインタフェースである。

【0033】バス117は、CPU101、ROM103、RAM105、ICカードR/W部107、第1LANI/F111、第2LANI/F113および外部I/O115間でデータが転送される経路である。

【0034】図3は、上記実施の形態に係るセキュアIFAXアダプタの主要な機能を示すブロック図である。信号種別判別部303は、IFAX端末21から電子メールアドレスを送信する処理において、第2LANI/F113から出力される所定のコマンド信号(応答信号)、または、LAN11~17から電子メールアドレスを受信する処理において、第1LANI/F111から出力される所定のコマンド信号(応答信号)の種別を判別する。所定のコマンド信号を判別した場合、信号種別判別部303は、第2LANI/F113および第1LANI/F111から続いて電子メールアドレスが出力されることを認識し、その旨をメールアドレス通信部301に通知する。

【0035】なお、所定のコマンド信号(応答信号)は、IFAX端末21から電子メールアドレスを送信する処理においては、メールサーバ9から出力される“354”という応答信号である。一方、LAN11~17から電子メールアドレスを受信する処理においては、メールサーバ9に対して出力した“RETR”の後にメールサーバ9から出力されるOKレスポンスである。

【0036】メールアドレス通信部301は、信号種別判別部303より、電子メールアドレスが出力される旨の通知を受けた場合に、第1LANI/F111および第2LANI/F113から電子メールアドレスを受信する。

また、メールアドレス通信部301は、後述するカード情報判定部305から受け取った電子メールアドレス情報に基づいて電子メールアドレスの送受信処理を行う。

【0037】カード情報判定部305は、ICカードスロット307に装着されたICカード109からICカードR/W部107が読み取った情報の内容を判定する。そして、ICカード109に署名処理または署名暗号化処理に必要な情報が格納されている場合に署名暗号化処理部309にその情報を与える。

【0038】また、カード情報判定部305は、ICカードR/W部107が読み取った情報に基づいてICカード109の装着の有無についても判定する。さらに、カード情報判定部305は、ICカード109に格納された電子メールアドレス情報を判定し、その電子メールアドレス情報をメールアドレス通信部301に通知する。

【0039】署名暗号化処理部309は、カード情報判定部305から受け取った署名暗号化処理等に必要な情報に基づいて、メールアドレス通信部301が受信した電子メールアドレスに対して署名暗号化処理等の処理を行う。また、署名暗号化処理部309は、カード情報判定部305から受け取った署名暗号化処理等に必要な情報に基づいて、メールアドレス通信部301が受信した電子メールアドレスに施された署名暗号化処理等の解読処理を行う。

【0040】ここで、ICカード109に格納された情報について説明する。ICカード109は、IFAX端末21から電子メールを送信する各ユーザが所有するものであり、各所有者に付与された電子メールアドレス情報(宛先アカウント)が格納されている。すなわち、セキュアIFAXアダプタ23にICカード109が装着されているときのみ、各所有者は、自分の電子メールアドレスから電子メールを送信することができ、自分の電子メールアドレスに対する電子メールを受信することができる。

【0041】また、ICカード109は、署名処理又は署名暗号化処理に必要な情報を格納する。すなわち、ICカード109は、自分の秘密鍵情報および公開鍵情報を格納する。なお、送信先の公開鍵情報は、証明書サーバ10から検索した後セキュアIFAXアダプタ23のRAM105内に蓄積される。

【0042】一方、IFAX端末21は、例えば、特開平8-242326号公報に開示されているような、スキャナで読み取った画像を電子メールに変換し、LANを介して送信すると共に、送信側で画像を変換した電子メールを受信し、元の画像に逆変換して印刷する装置という。IFAX端末21の具体例を図4を参照して簡単に説明する。図4は、上記実施の形態に係るセキュアIFAXアダプタに接続されるIFAX端末の構成を示すブロック図である。

【0043】IFAX端末21は、CPU401、RO

M403、RAM405に加えて、原稿をスキャンして画像を得るスキャナ部407、画像を例えばMHのような圧縮形式で圧縮画像データに圧縮し、逆に圧縮画像データを元の画像に伸長する圧縮・伸長部409と、セキュアIFAXアダプタ23などに接続するLANI/F413、画像を印刷するプリンタ部415、宛先を入力するためのパネル部411、圧縮画像データを電子メールに変換するフォーマット変換部419および電子メールを圧縮画像データに逆変換するフォーマット逆変換部421を具備する。

【0044】IFAX端末21では、送信者がスキャナ部407の原稿載置台に原稿をセットし、パネル部411から宛先メールアドレスを入力してスタートボタンを押すと、原稿を読み取って画像データを得、この画像データを圧縮・伸長部409で圧縮して圧縮画像データとする。この圧縮画像データをフォーマット変換部419によりMIMEに従って電子メールの添付ファイルとしてコーディングした電子メールに変換する。この電子メールをLANI/F413を介してセキュアIFAXアダプタ23へ送信する。

【0045】一方、IFAX端末21は、LANI/F413を介して電子メールを受信したならば、電子メールに添付された圧縮画像データをデコードし、圧縮・伸長部409で伸長し、元の画像データに復元し、プリンタ部415で印刷する。

【0046】本実施の形態では、上述のように送信側のIFAX端末21AおよびセキュアIFAXアダプタ23Aによって電子メール送信端末装置が、受信側のIFAX端末21BおよびセキュアIFAXアダプタ23Bによって電子メール受信端末装置が夫々構成されている。

【0047】図5は、上記実施の形態に係るメールサーバのハードウェア構成を示すブロック図である。メールサーバ9において、ネットワーク接続部501は、LAN11、13と接続するものである。メールボックス502は、ハードディスク等の二次記憶装置503内に設けられ、受信した電子メールアドレスを宛先ごとに記憶する。

【0048】CPU504は、コンピュータ等を動作させるものであり、RAM505、ROM506を用いて、受信した電子メールに対して図9に示す処理を行う。

【0049】宛先認識部507は、受信した電子メールアドレスの送信宛先を認識するものである。ここで送信宛先を認識できない場合、エラーメール作成部508に対してエラーメールの作成を指示する。

【0050】メールアドレス判断部509は、署名付きメールか否かにより電子メールアドレスの種別を判断し、署名付きメールであれば、着信メール作成部510に対して着信メールを作成させる。

【0051】POP受信要求判断部511は、端末からのPOP受信要求があったか、否かを判断し、その要求があれば、電子メールボックス502に対して、その要求者のアカウントに基づいて対応するメールアドレスを送信する。アカウント管理部512は、メールサーバ9が自ら管理する電子メール受信端末装置のアカウントを管理する。

【0052】以下、上記実施の形態に係る電子メール配信システムにおいて、本部Aから本部A1にそれぞれ設置したIFAX端末21およびセキュアIFAXアダプタ23間で電子メールを送受信した場合を例に挙げて説明する。

【0053】図6は、上記実施の形態に係る電子メール配信システムでのメール配信シーケンスを示す図である。図7は、上記実施の形態に係る電子メール配信システムでの送信側のセキュアIFAXアダプタの動作を示すフロー図である。図8は、上記実施の形態に係る電子メール配信システムでの送信側のIFAX端末でのメール送信動作を示すフロー図である。図9は、上記実施の形態に係る電子メール配信システムでのメールサーバのメール配信動作を示すフロー図である。図10は、上記実施の形態に係る電子メール配信システムでの受信側のセキュアIFAXアダプタの動作を示すフロー図である。

【0054】図6に示すように、本実施の形態による電子メール配信は、送信者がICカード109を送信側のセキュアIFAXアダプタ23AのICカードスロット307に挿入することから始まる。図7に示すように、ICカード109が挿入されると（ステップ（以下、STという）601）、証明書サーバ10に、ICカード109に記憶された証明書が有効か否かの確認を問い合わせる（ST602）。問い合わせ結果が有効であるか否か判定し（ST603）、有効であれば送信側のIFAX端末23Aからのメッセージの送信を待つ（ST604）。

【0055】なお、セキュアIFAXアダプタ23Aで、証明書の確認処理が完了するする前に、IFAX端末21Aからメッセージが送信される場合が考えられる。このときには、送信されたメッセージを、セキュアIFAXアダプタ23A内に一旦取り込んでおき、証明が確認された後に、自動的にメッセージ送信を行うようにする。この構成により、IFAX端末21AとセキュアIFAXアダプタ23Aとの間で、証明書確認のための通信を行う必要がなく、既存のIFAX端末を用いることができる。一方で、セキュアIFAXアダプタ23Aから確認処理が完了した旨の通知をIFAX端末21Aが受けると、IFAX端末21A側内で待機されたメッセージが送信されるようにしても良い。この構成では、セキュアIFAXアダプタ23Aにデータを取り込むことを必要としないため、余計なメモリを要せず、また確

認証が完了した後に、送信が実行がなされるため、確実な処理を行うことができるものである。

【0056】送信側のIFAX端末23Aでは、図8に示すように、パネル部411から宛先が指定された後（ST701）、パネル部411に設けられたスタートボタン（図示せず）が押し下げられると（ST702）、スキャナ部407で原稿を読み取り（ST703）、得られた画像データを圧縮・伸長部409で圧縮し（ST704）、フォーマット変換部419でTIFFフォーマットに変換し（ST705）、メッセージを作成する。このメッセージには宛先アドレスが含まれている。その後、メッセージをLANI/F413からセキュアIFAXアダプタ23Aに送信する（ST706）。

【0057】図7に戻って、ST604において、セキュアIFAXアダプタ23Aは、IFAX端末21Aからメッセージを受信したならば、メッセージから宛先アドレスを取得する（ST605）。この宛先アドレスを使って証明書サーバ10に宛先証明書を要求する（ST606）。証明書サーバ10はリポジトリ検索を行い、宛先証明書を発行する。リポジトリ検索とは、宛先アドレスから証明書サーバ10に保存されている宛先証明書を検索することをいう。セキュアIFAXアダプタ23Aは、証明書を取得したか否か判定し（ST607）、所得したならば、IFAX端末21Aから受信したメッセージに対して電子署名処理（ST608）、および暗号化処理（ST609）を施して、署名暗号化処理された電子メール（以下、「署名付メール」という）を作成する。

【0058】より具体的には、図3に示す署名暗号化処理部309が、証明書サーバ10からの宛先証明書（公開鍵情報）を入手する。一方、カード情報判定部305は、ICカード109に格納されている自己の秘密鍵情報を署名暗号化処理部309に渡す。署名暗号化処理部309は、この自己の証明書（秘密鍵情報）および宛先の証明書（公開鍵情報）を用いて署名暗号化処理を行う。

【0059】さらに詳細に説明すると、まずメッセージからハッシュ関数等の不可逆性の関数で演算処理を行い、メッセージダイジェストを取り出し、そのメッセージダイジェストに自己の秘密鍵情報を用いて暗号化処理を施す。さらに、DEK（DataEncryption Key）と呼ばれる擬似乱数を用いた暗号鍵を生成する。そして、そのDEKに対して送信先の公開鍵情報を用いて暗号化処理を施す。一方、先に暗号化処理を施したメッセージダイジェスト（署名結果）および電子メールのメッセージに対して、そのDEKで所定の暗号化方式（例えば、DES：Data Encryption Standard）にしたがって暗号化処理を施す。

【0060】ST607において宛先証明書を取得でき

ない場合には、IFAX端末21Aにエラーを通知し

（ST611）、処理を終了している。しかし、カード情報判定部305が、ICカード109に格納されている自己の秘密鍵情報を署名暗号化処理部309に渡し、署名暗号化処理部309は、この自己の秘密鍵情報を用いて署名処理を行うようにしても良い。

【0061】このようにして作成された署名付メールをメールサーバ9に宛てて送信し（ST610）、送信が正常に完了したか否か判定する（ST612）。正常に完了しない場合にはIFAX端末21Aにエラーを通知する（ST611）。

【0062】一方、ST603において、証明書が無効であった場合、表示モニタ27にICカードが無効である旨のメッセージを表示し（ST613）、IFAX端末21Aからメッセージ送信があったならば（ST614）、IFAX端末21Aにエラーを通知する（ST615）。

【0063】図8に戻って、送信側のIFAX端末21Aは、ST706でメッセージを送信した後、セキュアIFAXアダプタ23Aでエラーがあったか否かを監視し（ST707）、エラーがなければ送信が正常終了した旨のメッセージをパネル部411のLCD（図示せず）に表示し（ST708）、エラーがあればその旨を表示する（ST709）。

【0064】送信側のセキュアIFAXアダプタ23Aから署名付メールを含む、種々の電子メールをメールサーバ9が受信する。図9に示すように、メールサーバ9は、接続要求があったならば（ST801）、電子メール受信を行う（ST802）。これは例えばSMTPプロトコルにより行われる。電子メール受信でエラーが発生したか否か判定し（ST803）、エラーがあれば送信元にエラー通知メールを送信し（ST804）、処理を終了する。一方、エラーがなければ、電子メールの宛先アカウントを自らが管理しているか否か判定する（ST805）。宛先アカウントを管理していないならば、受信した電子メールを他のサーバに転送し（ST806）、処理を終了する。

【0065】自らが管理している宛先アカウントであれば、電子メールの種別を判定する（ST807）。判定は、具体的には、次のように行う。メールヘッダを解析して送達確認のヘッダ、すなわち“context-type:multipart/report:”があれば送達確認メールとみなす。

【0066】判定が終了したならば、判定の結果に基づいて電子メールが送達確認メールか否か判定する（ST808）。送達確認メールについては後述する。

【0067】送達確認メールでなかったならば、電子メールを宛先アカウントに対応するメールアダプタに格納する（ST809）。次いで、電子メールが署名付メールか否か判定し（ST810）、署名付メールであれば、その着信を受信側のセキュアIFAXアダプタ23

Bに通知する着信通知メールを作成する(ST811)。この着信通知メールは、署名付メールの宛先アカウント(宛先メールアドレス)と同一の宛先に宛てて送信するため、宛先フィールド[T o:]にはこの宛先アカウント(例えば、shibuty@shibu.co.jp)が指定されている。メールサーバ9は、DNSにより受信側のIFAXアダプタ23BのIPアドレスを認識し、これに宛ててSMTPプロトコルで着信通知メールを送信する(ST811)。

【0068】なお、署名付メールであるか否かの判断は、メールヘッダに記述されている“Content-type”の欄に“sign”の文字列があることで判断する。

【0069】受信側のセキュアIFAXアダプタ23Bは、メールサーバ9からのメール受信の要求を常時待っている(ST901)。要求があったならば着信通知メールをSMTPプロトコルで受信する(ST902)。その後、着信通知メールを解析し、その宛先アドレスを所有する個人(以下、単に「受信者」という)宛てに着信付メールが着信していることを通報する(ST903)。この通報方法は特に限定されないが、具体的には、表示モニタ27に着信通知のメッセージや受信者の名前を表示したり、スピーカ29から音声により受信者の名前やメッセージを再生したり、表示灯31を点灯させるなどにより行うことができる。この通報を受けて受信者はICカード109をセキュアIFAXアダプタ23Bのカードスロット307に挿入する。

【0070】受信側のセキュアIFAXアダプタ23Bは、ICカード109の挿入を確認したならば(ST904)、ICカード109の所有者情報と宛先とが一致するか否かを判定する(ST905)。宛先が一致しなかったならば、エラー表示を行い(ST906)、一致するまでST903~ST905を繰り返す。宛先が一致したならば、ICカード109から証明書を読み出し(ST907)、証明書サーバ10に対して証明書が有効か否かの確認を問い合わせる(ST908)。その結果に基づいて証明書が有効か否かを判断し(ST909)、有効であったならば、受信指示要求のメッセージを表示モニタ27に表示する(ST910)。無効であった場合には、エラー表示を行い(ST911)、処理を終了する。

【0071】受信者が受信側のIFAX端末21Bの受信指示ボタンをオンすると、セキュアIFAXアダプタ23Bに対して受信指示信号が送信される。この受信指示がIFAX端末21Bからあったならば(ST912)、セキュアIFAXアダプタ23Bは、メールサーバ9との間でPOP受信を行い、署名付メールを受信する(ST913)。このPOP受信には、ICカード109内に格納された受信者のログインIDおよびパスワードが用いられる。

【0072】セキュアIFAXアダプタ23Bは、受信

した署名付メールのデータを復号化する(ST914)。この復号化は、図3に示す署名暗号化処理部309が行う。具体的には、暗号化されているDEKを自分の秘密鍵情報で復号化し、復号化したDEKで暗号化されたデータを復号化する。そして、復号化したデータから、電子メールデータをメッセージダイジェストとメッセージデータに分離する。

【0073】次いで、この復号化でエラーが発生したか否かを判定し(ST915)、エラーがあったならば、エラー表示を行い(ST916)、処理を終了する。エラーがなく正常に復号化が行われたならば、証明書サーバ10から送信者の証明書(公開鍵情報)を取得する(ST917)。そして、取得した公開鍵情報を用いて署名検証を行う(ST918)。署名検証処理も、署名暗号化処理部309が行うが、具体的には、復号化処理で得たメッセージダイジェストを送信者の公開鍵情報で復号化し、その結果を保持しておく。また、復号化処理で分離したメッセージデータから、上述したようなハッシュ関数を用いてメッセージダイジェストを抽出する。そして、そこで得たメッセージダイジェストと先ほど保持したメッセージダイジェストとを比較する。これにより、電子メールのメッセージデータが改ざんされていないか、また、正当な送信者から送信されたかを確認することができる。

【0074】このような署名検証でエラー(すなわち、正当な送信者から改ざんなくメッセージが送信されていない)が起こったか否かを判定し(ST919)、エラーがあったならばその旨を表示モニタ27に表示して(ST920)、処理を終了する。エラーがなかったならば、復号化したデータをIFAX端末21Bに送信して印刷、表示などを行わせる(ST921)。次いで、送達確認メールを作成し、メールサーバ9にSMTP送信する(ST922)。

【0075】メールサーバ9は、送達確認メールを受信した場合、図9のST808において送達確認メールであることを認識し、送信元にSMTPプロトコルで転送する(ST813)。送達確認メールは、図6のシーケンス図に示すように、SMTPプロトコルを用いて受信側のセキュアIFAXアダプタ23B、メールサーバ9、送信側のセキュアIFAXアダプタ23Aを順次経由して、送信側のIFAX端末21Aが受信し、送達レポートとして表示、印刷などで出力する。また、送信側のセキュアIFAXアダプタ23Aは、送達確認メールを受信したならばその旨を履歴管理サーバ7に登録する。

【0076】以上説明したように、本実施の形態によれば、メールサーバ9は、署名付メール(すなわち、署名処理および暗号化が施された電子メール)を受信したならば、署名付メールの受信者が登録された受信側のセキュアIFAXアダプタ23Bに対して着信通知メールを

送信し、受信側のセキュア I F A X アダプタ 2 3 B は、着信通知メールを受信したならばその宛先アカウントからその所有者である受信者に対して暗号化メールの着信を通報し、I C カード 1 0 9 を用いて受信者の個人認証を行うことを要求し、受信者の確認が取れた後署名付メールを受信、復号化するので、署名付メールの機密文書をメールサーバ 9 から所望の受信者に迅速かつ確実に取り出させることができる。この結果、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができる。

【0077】また、送信側のセキュア I F A X アダプタ 2 3 A では、I C カード 1 0 9 を用いて証明書サーバ 1 0 に証明書の有効性を確認することで個人認証を行い、送信者の確認を取った後、電子メールを署名処理および暗号化を施して宛先に送信するので、不正な送信者による機密文書の配信を未然に防止することができる。

【0078】また、受信側のセキュア I F A X アダプタ 2 3 B は、署名付メールを正常に受信したならば、送達確認通知を送信側に返し、送信側の I F A X 端末 2 1 A はこれを印刷したり、送信履歴を履歴管理サーバ 7 に登録するので、機密文書の配信があったことを送信者が確認したり、その後第三者などが送信履歴を容易に確認することができる。

【0079】上述の本実施の形態では、I F A X の基本的構成（画情報を電子メールで送受信する構成等）とセキュア I F A X の拡張部分構成（署名処理・暗号化処理等）とが別々の装置により実現されているが、これに限定されるものではなく、I F A X 端末 2 1 がセキュア I F A X アダプタ 2 3 の機能を内蔵していても良い。

【0080】また、本実施の形態では、個人認証に I C カード 1 0 9 に記憶された証明書を証明書サーバ 1 0 で確認することで行っているが、これに代わって、音声認証、指紋認証等の他の一般的に知られている個人認証技術を用いても良いし、これと併有しても良い。しかしながら、本実施の形態で採用する I C カードを用いた個人認証は、公用鍵を用いた暗号化および秘密鍵による復号化を可能とする点で優れている。

【0081】また、本実施の形態では、電子メールに署名処理および暗号化処理を施しているが、署名処理を行わず単に暗号化のみということもできる。よって、本発明は広く暗号化を施した電子メール、すなわち暗号化メールによる機密文書の配信に関するものである。

【0082】本発明は、当業者に明らかなように、上記実施の形態に記載した技術にしたがってプログラムされた一般的な市販のデジタルコンピュータおよびマイクロプロセッサを使って実施することができる。また、当業者に明らかなように、本発明は、上記実施の形態に記載した技術に基づいて当業者により作成されるコンピュータプログラムを包含する。

【0083】また、本発明を実施するコンピュータをプ

ログラムするために使用できる命令を含む記憶媒体であるコンピュータプログラム製品が本発明の範囲に含まれる。この記憶媒体は、フロッピー（登録商標）ディスク、光ディスク、CD-ROM および磁気ディスク等のディスク、ROM、RAM、EPROM、EEPROM、磁気光カード、メモリカードまたは DVD 等であるが、特にこれらに限定されるものではない。

【0084】

【発明の効果】以上説明したように本発明によれば、電子メールサーバ装置は暗号化メールを受信したならば、暗号化メールの受信者が登録された受信側の電子メール受信端末装置に対してその着信を通知する着信通知メールを送信し、電子メール受信端末装置は、着信通知メールを受信したならばその宛先アカウントからその所有者である受信者に対して暗号化メールの着信を通報し、受信者の個人認証を行うことを要求し、受信者の確認が取れた後暗号化メールを受信、復号化するので、暗号化メールの機密文書を電子メールサーバ装置から所望の受信者に迅速かつ確実に取り出させることができる等効果を奏するものである。

【図面の簡単な説明】

【図 1】本発明の一実施の形態に係る電子メール配信システムを示す概念図

【図 2】上記実施の形態に係るセキュア I F A X アダプタのハードウェア構成を示すブロック図

【図 3】上記実施の形態に係るセキュア I F A X アダプタの主要な機能を示すブロック図

【図 4】上記実施の形態に係るセキュア I F A X アダプタに接続される I F A X 端末の構成を示すブロック図である。

【図 5】上記実施の形態に係るメールサーバのハードウェア構成を示すブロック図

【図 6】上記実施の形態に係る電子メール配信システムでのメール配信シーケンスを示す図

【図 7】上記実施の形態に係る電子メール配信システムでの送信側のセキュア I F A X アダプタの動作を示すフロー図

【図 8】上記実施の形態に係る電子メール配信システムでの送信側の I F A X 端末でのメール送信動作を示すフロー図

【図 9】上記実施の形態に係る電子メール配信システムでのメールサーバのメール配信動作を示すフロー図

【図 10】上記実施の形態に係る電子メール配信システムでの受信側のセキュア I F A X アダプタの動作を示すフロー図

【符号の説明】

1 電子メール配信システム

7 履歴管理サーバ

9 メールサーバ

10 証明書サーバ

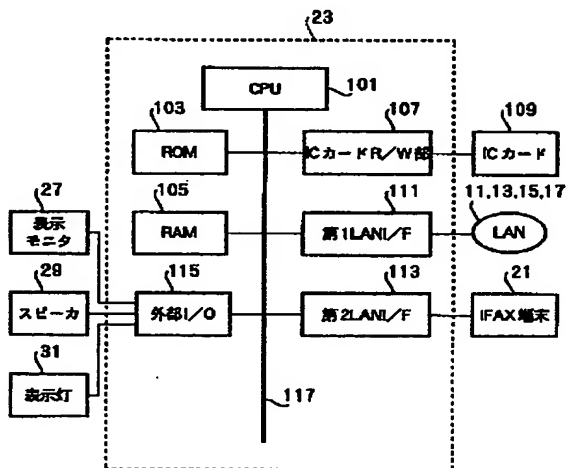
17

18

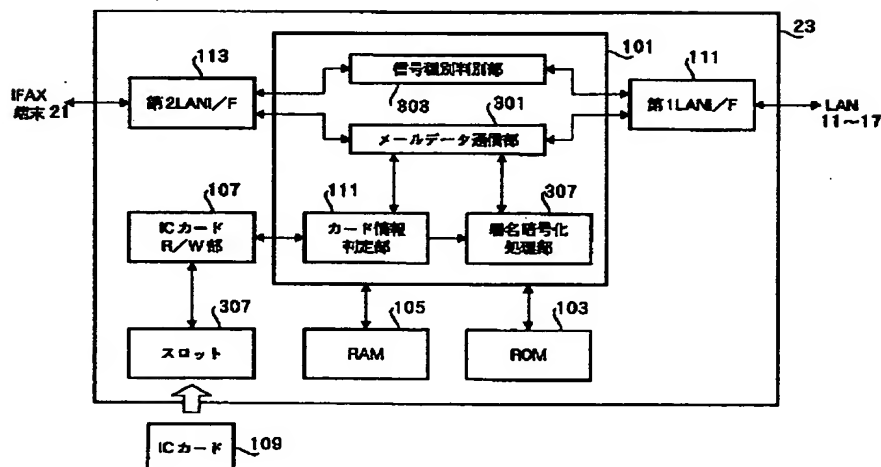
21、21A、21B IFAX端末
 23、23A、23C セキュアIFAXアダプタ
 27 表示モニタ
 29 スピーカ
 31 表示灯
 107 ICカードR/W部
 109 ICカード
 301 メールデータ通信部
 303 信号種別判別部
 305 カード情報判定部
 307 カードスロット
 309 署名暗号化処理部
 407 スキャナ部
 409 圧縮・伸長部
 411 パネル部

415 プリンタ部
 419 フォーマット変換部
 421 フォーマット逆変換部
 501 ネットワーク接続部
 502 メールボックス
 503 二次記憶装置
 504 CPU
 505 RAM
 506 ROM
 10 507 宛先認識部
 508 エラーメール作成部
 509 メールデータ判断部
 510 着信メール作成部
 511 POP受信要求判断部
 512 アカウント管理部

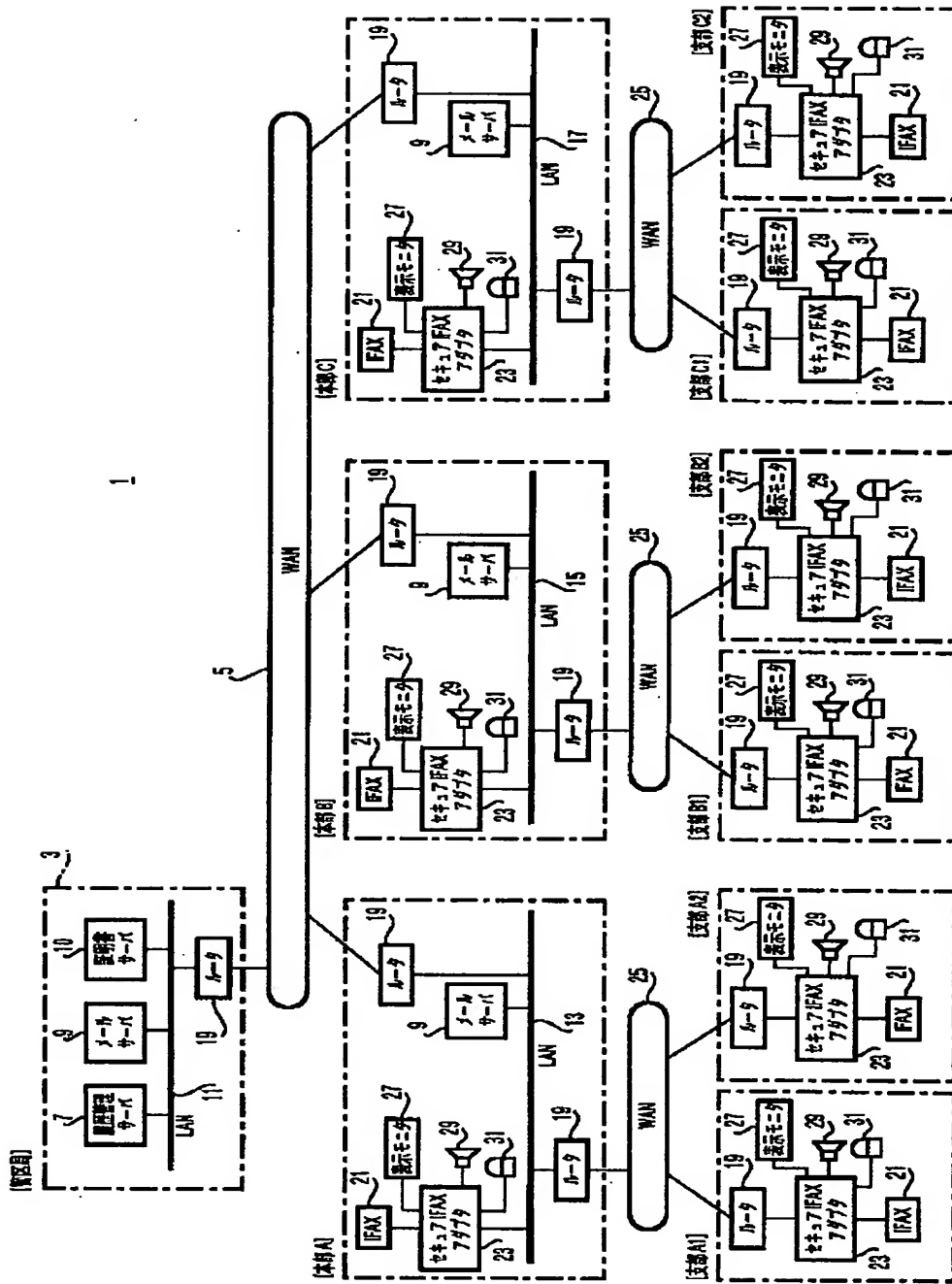
【図2】



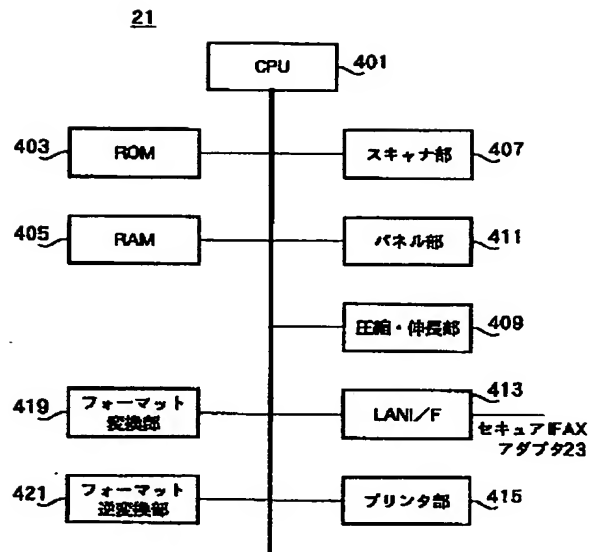
【図3】



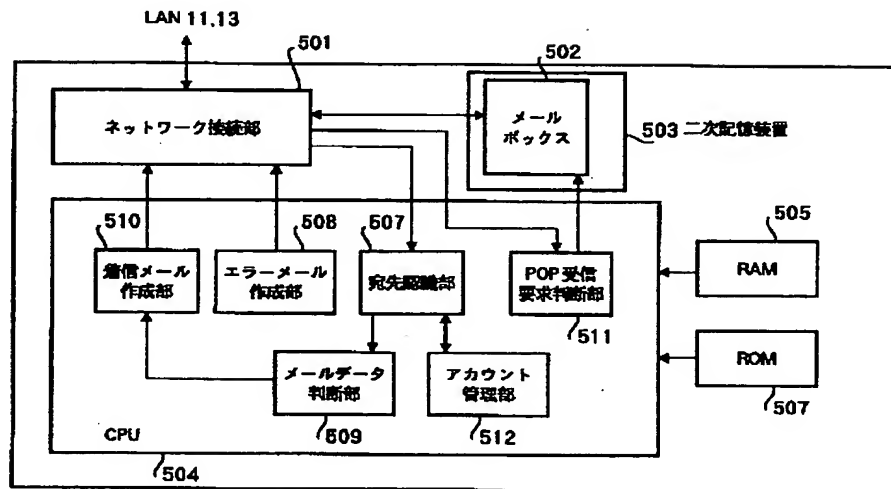
【図 1】



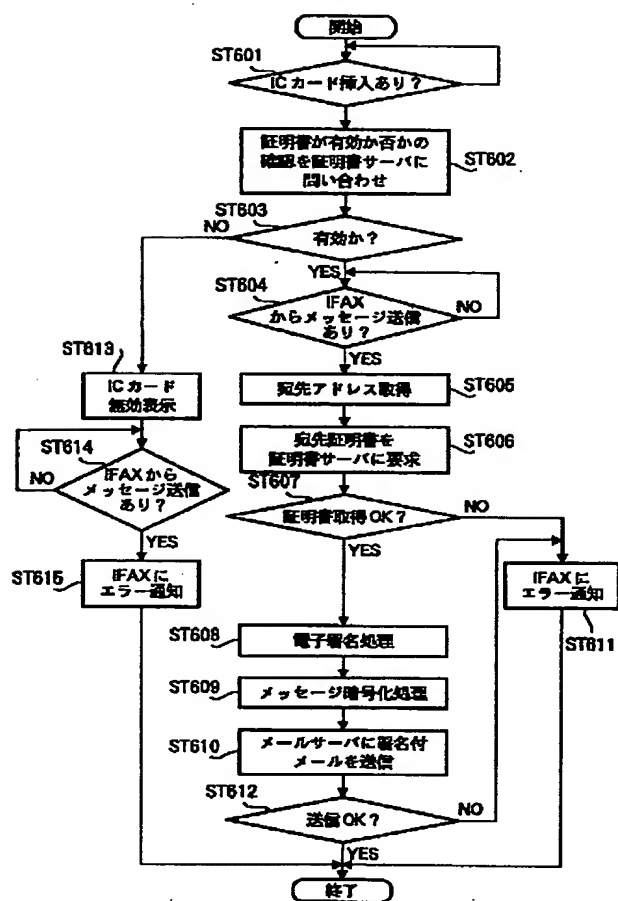
【図 4】



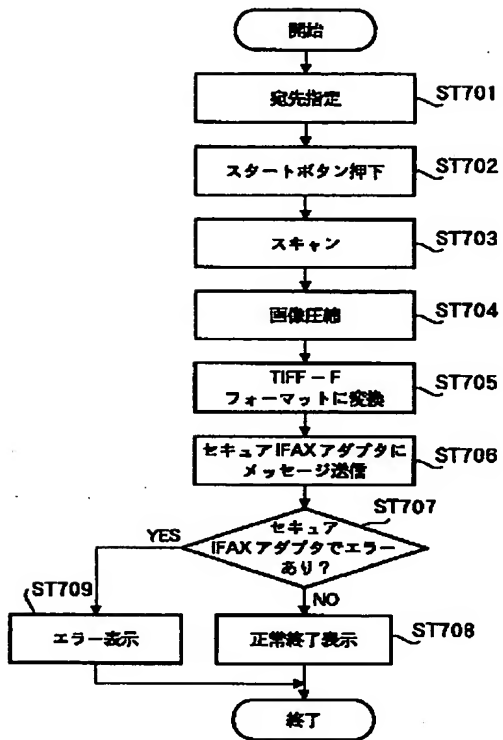
【図 5】



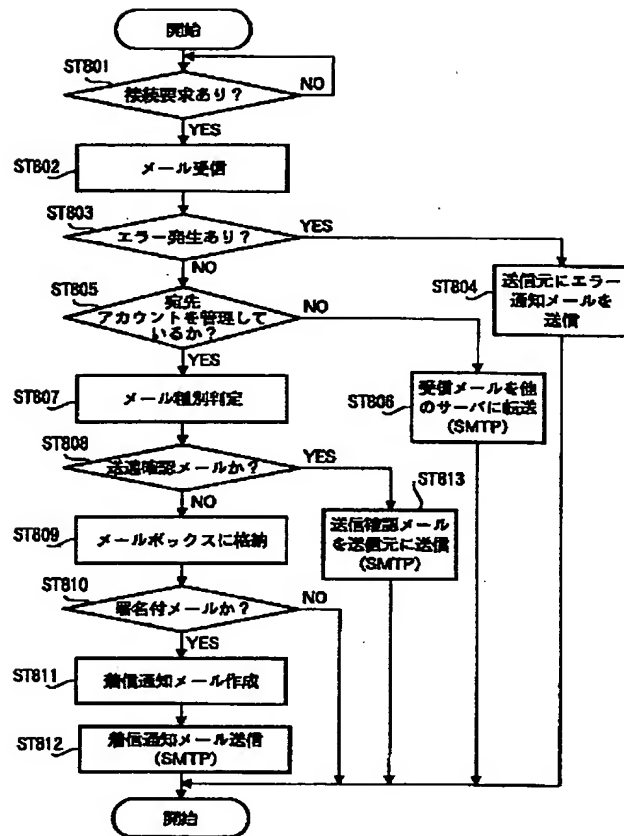
【圖 7】



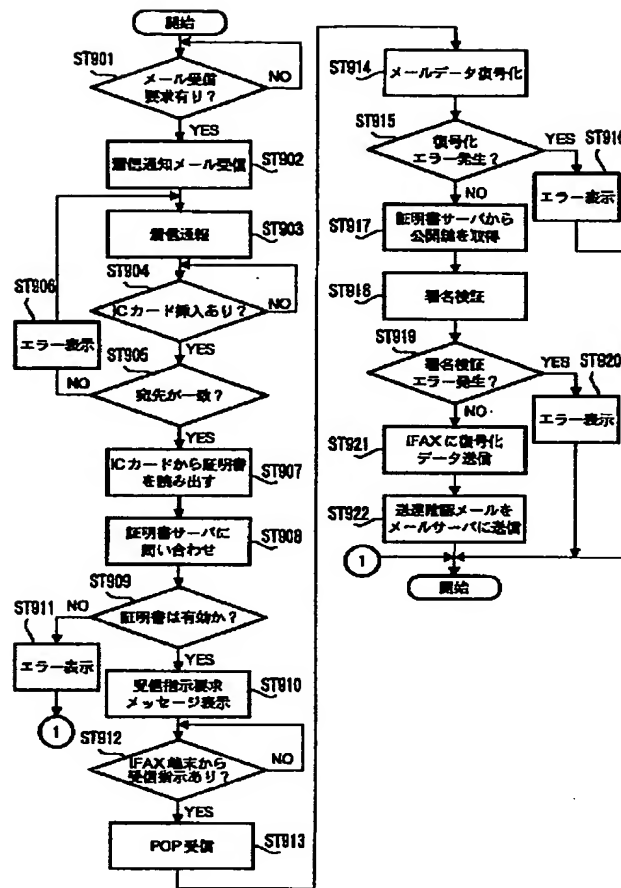
【図 8】



【図 9】



【図 10】



フロントページの続き

(51) Int. Cl.⁷
H04N 1/44

識別記号

F I
H04N 1/44

テーマコード (参考)

(72) 発明者 秋元 正男
東京都目黒区下目黒2丁目3番8号 松下
電送システム株式会社内Fターム (参考) 5C062 AA02 AA21 AA29 AA35 AB38
AC38 AF00 BD09
5C075 AB90 CB90 CF04 EE03 EE06
5K030 GA15 HA06 LD13 LD20

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.